

CASE C-362/14

MAXIMILLIAN SCHREMS

Applicant

V.

DATA PROTECTION COMMISSIONER

Respondent

AND

DIGITAL RIGHTS IRELAND LIMITED

Amicus curiae

Annex A.1

Opinion on the adequacy of the Safe Harbor Decision, Prof. Dr.
Franziska Böhm

WESTFÄLISCHE WILHELMS-UNIVERSITÄT
Institute for Information-, Telecommunication- and Media-Law (ITM)
Prof. Dr. Franziska Boehm
Assistant Professor for IT-Law

Opinion on the adequacy of the Safe Harbor Decision

November 9
2014

Comparison between Safe Harbor
and Directive 95/46

Content

| | |
|---|----|
| I. APPLICATION OF SAFE HARBOR | 4 |
| 1. Scope | 4 |
| a) General Remarks | 4 |
| b) Result of Comparison | 4 |
| 2. Applicable Law | 5 |
| a) General Remarks | 5 |
| b) Result of Comparison | 6 |
| 3. Exceptions and Restrictions | 6 |
| a) General Remarks | 6 |
| b) Result of Comparison | 8 |
| 4. Summary Application | 8 |
| II. SUBSTANTIVE LAW GUARANTEES | 9 |
| 1. Data Quality | 9 |
| a) General Remarks | 9 |
| b) Result of Comparison | 11 |
| 2. Legitimate Processing | 11 |
| a) General Remarks | 11 |
| b) Result of Comparison | 12 |
| 3. Onward Transfer | 14 |
| a) General Remarks | 14 |
| b) Result of Comparison | 15 |
| 4. Summary Substantive Law Guarantees | 15 |
| III. RIGHTS OF DATA SUBJECTS | 16 |
| 1. Right to Access/Erasure/Rectification/Blocking | 16 |
| a) General Remarks | 16 |
| b) Result of Comparison | 18 |
| 2. Information Duties | 18 |
| a) General Remarks | 18 |
| b) Result of Comparison | 19 |
| 3. Summary Rights of the Data Subject | 19 |
| IV. ENFORCEMENT | 20 |
| 1. Remedies | 20 |
| a) General Remarks | 20 |
| b) Result of Comparison | 21 |
| 2. Notification/Prior Checking/Publicizing | 22 |
| a) General Remarks | 22 |
| b) Result of Comparison | 23 |
| 3. Supervisory Authority/Enforcement | 24 |
| a) General Remarks | 24 |
| b) Result of Comparison | 25 |
| 4. Sanctions | 26 |
| a) General Remarks | 26 |
| b) Result of Comparison | 27 |
| 5. Summary Enforcement | 27 |
| V. FINAL REMARKS | 29 |

Abbreviations used in the opinion

CFR = Charter of Fundamental Rights of the European Union

Communication of the Commission on the functioning of SH =

Communication from the Commission to the European Parliament and the Council on the functioning of the Safe Harbour from the Perspective of EU Citizens and Companies Established in the EU of 27th of November 2013, Com(2013) 847

Directive 95/46 = Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, OJ 1995, L 281/31

ECHR = European Convention on Human Rights

ECtHR = European Court of Human Rights

SH = Safe Harbor

SHD = Commission Decision of 26 July 2000 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequacy of the protection provided by the safe harbour privacy principles and related frequently asked questions issued by the US Department of Commerce, OJ 2000, L 215/7

US = United States

Other abbreviations relating to specific measures are explained in the text.

The opinion includes a brief comparison between the basic data protection guarantees of Directive 95/46 and the guarantees stipulated by the Safe Harbor Decision (SHD in the following). It should give a quick overview of the most important data protection principles in both instruments and serve as background information for the written observations.

Starting point for the opinion are the provisions of Directive 95/46 allowing the transfer of personal data of EU citizens to a third state. For this purpose, Article 25 (1) of Directive 95/46 requires an adequate level of protection in the third country. The directive does not require an equivalent level of protection, meaning that the guarantees in the third country can differ from the data protection guarantees in the EU to a certain degree. The difference in the wording leaves a certain leeway for the Commission to accept an adequate level of protection in a third country although the data protection guarantees in the third country do not meet exactly the same level as those in the EU. Nonetheless, it is clear that the adequacy decision of the Commission requires the respect of basic data protection guarantees.

When assessing the adequacy, the following criteria stipulated in Article 25 (2) of Directive 95/46 play a role: “the circumstances surrounding a data transfer operation or set of data transfer operations; the nature of the data, the purpose and duration of the proposed processing operation or operations, the country of origin and country of final destination, the rules of law, both general and sectoral, in force in the third country in question and the professional rules and security measures which are complied with in that country”.

It results from the wording of Article 25 (1) and (2) that they are designed to enable adequacy decisions for entire countries. However, as the data protection framework in the US as an entire country could not be assessed as adequate, a specific regime, the SHD, was put in place to enable data transfer in specific situations. This special legal nature of the SHD leaves however no doubt on the general applicability of basic data protection principles.

The following analysis is not intended to be exhaustive. It focuses on a comparison of the most important EU data protection principles that are illustrated by means of comparative tables.

I. APPLICATION OF SAFE HARBOR

1. Scope

a) General Remarks

Directive 95/46 has a broad application to all private and public “controllers” of personal data within the EU. Only activities that fall outside of the scope of Community Law (e.g. states security, law enforcement and defence) are not governed by Directive 95/46 under Article 3, but will usually be governed by the ECHR, CFR and/or national constitutional laws of the EU member states.

In contrast to the wide application of Directive 95/46, the self-certification system of Safe Harbor (SH in the following) only applies to certified organizations established in the United States. This means that contrary to Directive 95/46, all government authorities and all non-certified organizations in the United States are outside of the SH system. As soon as data is transferred to a non-certified entity, the SH rules do not apply anymore (see “transfer” below).

| Directive 95/46 | Safe Harbor |
|---|--|
| Article 3 Scope 1. This Directive shall apply to the processing of personal data wholly or partly by automatic means, and to the processing otherwise than by automatic means of personal data which form part of a filing system or are intended to form part of a filing system. 2. This Directive shall not apply to the processing of personal data: - in the course of an activity which falls outside the scope of Community law, such as those provided for by Titles V and VI of the Treaty on European Union and in any case to processing operations concerning public security, defence, State security (including the economic well-being of the State when the processing operation relates to State security matters) and the activities of the State in areas of criminal law, [...] | Third Paragraph Decisions by organizations to qualify for the safe harbor are entirely voluntary, and organizations may qualify for the safe harbor in different ways. [...] |
| <i>[See also Articles 1, 2 and 4 of Directive 95/46 for the application of the Directive.]</i> | Fifth Paragraph Organizations may wish for practical or other reasons to apply the Principles to all their data processing operations, but they are only obligated to apply them to data transferred after they enter the safe harbor. [...] |

b) Result of Comparison

While Directive 95/46 generally applies to a range of private and public processing operations in the EU/EEA, the SH rules only apply to the US entities that have self-certified. Currently, the list includes more than 3800 companies. As the self-certification mechanism is not designed for the public sector, government authorities are not on the SH list. In this context, it should be briefly mentioned that SH is the first instrument with which a “sectoral self-certification” mechanism is found to be adequate. This can conflict with Article 25 Directive 95/46, which wording refers to a (whole) country (not a certificate)

to be found “adequate”. The only other existing adequacy decision referring to only one specific sector of a country is a second US-related decision, concerning the transfer of flight passenger data.¹

Further, if SH data is transferred to a public or private entity under a legal obligation or else resulting from US law, there is no subsequent protection following from the SH mechanism. While in the EU, individuals concerned by data processing operations are not only protected by the regime of Directive 95/46, but also by human rights and/or constitutional protection, if data is transferred outside of the scope of Directive 95/46, there is almost no protection available in the US for EU data that have been transferred to the US under the SH regime and that are then transferred to an organization not participating in the SH mechanism. Constitutional protection and protection according to the US privacy act of 1974 are only available to “US persons” (US citizens and legal permanent residence) in the United States.²

2. Applicable Law

a) General Remarks

Directive 95/46 is to be interpreted within EU law and primary legislation, such as Articles 7 and 8 CFR and Article 8 ECHR.

Following the system of US self-certification, the SH principles and Frequently Asked Questions are governed and interpreted under US law. In consequence, in cases of doubts relating to the interpretation and applicability of data protection principles in the framework of SH, only US law applies. Only if a US organization has submitted itself to the jurisdiction of a European Data Protection Authority, its data processing activities are to be interpreted under EU law.

| Directive 95/46 | Safe Harbor |
|--|---|
| Article 4, National law applicable 1. Each Member State shall apply the national provisions it adopts pursuant to this Directive to the processing of personal data where: (a) the processing is carried out in the context of the activities of an establishment of the controller on the territory of the | Sixth Paragraph U.S. law will apply to questions of interpretation and compliance with the Safe Harbor Principles (including the Frequently Asked Questions) and relevant privacy policies by safe harbor organizations, except where organizations have committed to cooperate with European Data Protection |

¹ Compare overview of the adequacy decisions: http://ec.europa.eu/justice/data-protection/document/international-transfers/adequacy/index_en.htm#h2-12.

² Compare for instance: Bowden, “The US surveillance programmes and their impact on EU citizens' fundamental rights” study requested by the European Parliament's Committee on Civil Liberties, Justice and Home Affairs in September 2013, p. 20, para 2.2.3, available at: http://www.europarl.europa.eu/RegData/etudes/note/join/2013/474405/IPOL-LIBE_NT%282013%29474405_EN.pdf and Privacy Act of 1974 (Pub.L. 93–579, 88 Stat. 1896, enacted December 31, 1974, 5 U.S.C. § 552a) together with the proposal to extend the privacy protections of the Privacy Act of 1974 to non-U.S. Persons in the recent report of the executive office of the president, “Big Data: seizing opportunities, preserving values” of May 2014, p. 60, available at: http://www.whitehouse.gov/sites/default/files/docs/big_data_privacy_report_may_1_2014.pdf.

| | |
|--|---|
| <p>Member State; when the same controller is established on the territory of several Member States, he must take the necessary measures to ensure that each of these establishments complies with the obligations laid down by the national law applicable;</p> <p>(b) the controller is not established on the Member State's territory, but in a place where its national law applies by virtue of international public law;</p> <p>(c) the controller is not established on Community territory and, for purposes of processing personal data makes use of equipment, automated or otherwise, situated on the territory of the said Member State, unless such equipment is used only for purposes of transit through the territory of the Community.</p> <p>2. In the circumstances referred to in paragraph 1 (c), the controller must designate a representative established in the territory of that Member State, without prejudice to legal actions which could be initiated against the controller himself.</p> | <p>Authorities. Unless otherwise stated, all provisions of the Safe Harbor Principles and Frequently asked Questions apply where they are relevant.</p> |
|--|---|

b) Result of Comparison

While Directive 95/46 must be interpreted in line with higher ranking law (e.g. the CFR and the ECHR)³, the SH is subject to US interpretation, US laws and the US constitution, which are not granting privacy protection for "non-US persons".⁴ For instance, the protection of the guarantees resulting from the 4th Amendment to the US Constitution is limited to US citizens.⁵ This leads to a very limited privacy protection of EU citizens in the US, even if data are transferred in the framework of SH.

3. Exceptions and Restrictions

a) General Remarks

Article 13 of Directive 95/46 includes a number of limitations and restrictions to the application of five Articles of the Directive. Such limitations are usually to be interpreted narrowly and limited by national constitutional laws, the ECHR and the CFR.⁶ SH includes the same limitations and restrictions by referring to Directive 95/46 in subparagraph (c) of the fourth paragraph of the SHD. EU law requires that such restrictions are provided for by a law that fulfils certain minimum requirements, such as accessibility,

³ Compare Boehm/Cole, Data Retention after the Judgement of the Court of Justice of the European Union, p. 23 et seq., available at: http://www.uni-muenster.de/Jura.itm/hoeren/materialien/boehm/Boehm_Cole-Data_Retention_Study-June_2014.pdf.

⁴ Bowden, The US surveillance programmes and their impact on EU citizens' fundamental rights, p. 19.

⁵ Bowden, The US surveillance programmes and their impact on EU citizens' fundamental rights, p. 20.

⁶ Brühann, in: Grabitz/Hilf, Das Recht der Europäischen Union, 40. Auflage 2009, Sekundärrecht, Teil A 30, Kapitel II, Abschn. VI, Art. 13, Rn. 1. Compare: ECtHR, Rotaru v. Romania, no. 28341/95, para. 47; CJEU, C-293/12 Digital Rights Ireland and 594/12 Seitlinger and Others.

foreseeability and clear and precise rules with regard to the circumstances justifying a limitation.⁷ Article 52 (1) of the CFR further requires that limitations and restrictions to the fundamental rights of the CFR respect the essence of the rights and are subject to the principle of proportionality. Further, “limitations may be made to those rights and freedoms only if they are necessary and genuinely meet objectives of general interest recognized by the Union or the need to protect the rights and freedoms of others.”⁸

In addition to the limitations that exist in Directive 95/46, the SH adds further exceptions in its fourth paragraph, subparagraphs (a) and (b). The limitation clarifies that any law, government regulation and case law override the self-certification mechanism. In addition all national security, public interest and law enforcement requirements make the SH non-applicable, even if they are not specified in a law, government regulation or case law. The US understanding of this exception is further explained in Annex IV of the SHD, which states that not only a duty to provide data, but also a “special authorization”, for instance, to share data, overrides the SH principles. This means in practice that any form of US statute/executive regulation can add further limitations to the ones provided for in Directive 95/46. In consequence, SH principles only apply when there is no other specific regulation within the US legal system.

| Directive 95/46 | Safe Harbor |
|---|---|
| Article 13, Exemptions and Restrictions 1. Member States may adopt legislative measures to restrict the scope of the obligations and rights provided for in Articles 6 (1), 10, 11 (1), 12 and 21 when such a restriction constitutes a necessary measures to safeguard: (a) national security; (b) defence; (c) public security; (d) the prevention, investigation, detection and prosecution of criminal offences, or of breaches of ethics for regulated professions; (e) an important economic or financial interest of a Member State or of the European Union, including monetary, budgetary and taxation matters; (f) a monitoring, inspection or regulatory function connected, even occasionally, with the exercise of official authority in cases referred to in (c), (d) and (e); (g) the protection of the data subject or of the rights and freedoms of others. | Fourth Paragraph Adherence to these Principles may be limited: (a) to the extent necessary to meet national security, public interest, or law enforcement requirements; (b) by statute, government regulation, or case law that create conflicting obligations or explicit authorizations, provided that, in exercising any such authorization, an organization can demonstrate that its non-compliance with the Principles is limited to the extent necessary to meet the overriding legitimate interests furthered by such authorization; or (c) if the effect of the Directive of Member State law is to allow exceptions or derogations, provided such exceptions or derogations are applied in comparable contexts. ANNEX IV B. Explicit Legal Authorizations [...]Clearly, where U.S. law imposes a conflicting obligation, U.S. organizations whether in the safe harbor or not must comply with the law. As for explicit authorizations, while the safe harbor principles are intended to bridge the differences between the U.S. and European regimes for privacy protection, we owe deference to the legislative prerogatives of our elected lawmakers. [...] The exception is limited to cases where there is an explicit authorization. Therefore, as a threshold matter, the relevant |

⁷ ECtHR, *S. and Marper v. UK*, no. 30562/04 and 30566/04, para. 95; *Copland v. UK*, no. 62617/00, para. 46; *Amann v. Switzerland*, no. 27798/95, para. 55.

⁸ CJEU, *C-293/12 Digital Rights Ireland and 594/12 Seitlinger and Others*, para. 38; Compare *Boehm/Cole, Data Retention after the Judgement of the Court of Justice of the European Union*, p. 34.

| |
|---|
| statute, regulation or court decision must affirmatively authorize the particular conduct by safe harbor organizations. |
|---|

b) Result of Comparison

The US constitution as well as most US laws and regulations do not grant a right to privacy to “non-US persons”. In contrast, it is clear from the wording of Annex IV of the SHD that every rule in form of “explicit legal authorizations” (from the federal, state or even the local level) existing in the US can override the guarantees of the SHD. As a result, in particular the provisions of Annex IV are capable of broadly restricting the rights of the persons whose data have been transferred.

In addition to Annex IV there is an exception for “national security”, “law enforcement” and “public interest”. It is not clear from the wording of this exception whether these restrictions require any basis in a law or regulation. This could mean that even a local town ordinance in the US can override SH. In essence, it is highly likely that SH principles are only applicable in a small number of situations. If however, the SH principles are not applicable, there is no chance of balancing the conflicting interests, as it would be required by EU law, if fundamental rights are restricted.⁹ An example is the current situation regarding the “PRISM” program: The FISA Act (50 U.S.C. Chapter 36, § 1801 et seq.) is overriding the SH rules and leaves non-US data subjects with no protection against mass surveillance by US espionage, national security and law enforcement authorities.¹⁰

In summary, in particular Annex IV of the SHD allows for restrictions and limitations of the fundamental rights of EU citizens which go far beyond of what is tolerated in the EU. The restrictions that are possible according to the SHD decision do not even require a proportionality or balancing test between the different interests at stake. This constitutes a clear violation of Article 7, 8 and 52 (1) CFR and the ECHR and can therefore not be regarded as adequate.

4. Summary Application

With regard to the scope of protection, it can be concluded that the scope of SH is very narrow and includes only the about 3.800 organizations that have “self-certified”. If SH data is transferred to organizations which are not subject to the SH rules, constitutional protection or protection following from other legal sources for data of EU citizens is almost non-existent. Privacy and data protection rules in the US differ significantly from the protection guaranteed in the EU. There are no general privacy or data protection laws in the US and constitutional protection of privacy for “non-US persons” is not provided for. Sectoral regulations govern certain aspects of privacy and data protection in a particular context (for instance Health Data, Online Data of Children, Credit Information).

In consequence, protection resulting from US laws and regulations is often weaker than in the EU, in particular for EU citizens. An example is the FISA Act (e.g. 50 U.S.C. Chapter 36, § 1881a) which only

⁹ See for example Article 52(1) CFR; Compare Boehm/Cole, Data Retention after the Judgement of the Court of Justice of the European Union, p. 34 et seq.

¹⁰ Bowden, The US surveillance programmes and their impact on EU citizens’ fundamental rights, p. 19 et seq.

grants US citizens and permanent residents protection but not EU citizens.¹¹ The difference regarding the standard of protection is also the reason why the US as a country is not qualified as a country providing “adequate protection” in the sense of Directive 95/46. In summary, the SH rules enable a wide ranging use of data outside the “sphere of protection” of SH. Circumventing the SH principles by transferring SH data to government authorities or other third parties – where lower data protection principles apply (if at all) – is easily possible. This clearly contradicts to EU data protection principles according to which strict data protection rules apply during the entire course of data processing.¹² It is therefore extremely doubtful whether the current SH mechanism can be regarded as providing an adequate protection.

In addition to the weak protection outside of the SH framework, the SH rules do not apply if there is US law overriding the application of the SH principles. This US law can include federal, state and local laws, case-law, regulations and even public interests that need no legal specification. Other explicit “authorizations” may even limit the scope further. Moreover, the rules of SH are subject to US interpretation. This weakens the standard of protection for SH data even more, since US privacy and data protection standards differ to a great extent from those of the EU (compare above).

II. SUBSTANTIVE LAW GUARANTEES

1. Data Quality

a) General Remarks

According to EU law “data quality” requirements constitute a central limitation for every kind of data usage.¹³ Directive 95/46 requires in its Article 6 the adherence to several principles when it comes to data processing. First, the processing must be fair and lawful. Secondly, according to the purpose limitation principle the collection of data may only take place for specified, explicit and legitimate purposes and further processing, incompatible to those purposes, is prohibited. Thirdly, the (limited) purpose requires that data processing must be adequate, relevant and not excessive. Accuracy and correctness of data is also required, which means that there have to be certain safeguards to get inaccurate or incomplete data erased or rectified. Finally, Directive 95/46 contains a limitation which concerns the extent of the data and demands that data is kept in a form which permits identification of data subjects for no longer than necessary. Each of the principles is not only important as a single principle; they also have a considerable meaning in their entirety. The more general idea of data minimization can be derived from them.¹⁴

¹¹ Ibid.

¹² Compare CJEU, C-293/12 Digital Rights Ireland and 594/12 Seitlinger and Others, paras. 32, 35.

¹³ Compare Handbook on European data protection law, chapter 3 (http://www.echr.coe.int/Documents/Handbook_data_protection_ENG.pdf); Brühann, in: Grabitz/Hilf, Art. 6 Rn. 6.

¹⁴ Compare for instance, European Data Protection Supervisor, <https://secure.edps.europa.eu/EDPSWEB/edps/lang/en/EDPS/Dataprotection/Glossary/pid/74>.

This idea as well as the specific principles that limit data processing can be found in primary EU law. Article 8 (2) CFR reiterates largely the rules laid down in Article 6 of Directive 95/46.¹⁵ Article 8 ECHR and the case law of the ECtHR with regard to this article regularly refer to the above-mentioned quality requirements.¹⁶ The same principles can be found in the "OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data"¹⁷ and the "Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data"¹⁸ of the Council of Europe. The mentioning of these principles in several sources of law and the reference in case law show their high acceptance even beyond mere EU law.

Data quality principles, respectively "data integrity" principles, are laid down in the SHD as well. The purpose limitation principle constitutes the core part. Besides, to ensure reliability of data, the SHD requires accurateness, completeness and correctness of data. The access principle refers to these safeguards.

| Directive 95/46 | Safe Harbor |
|--|---|
| Article 6, PRINCIPLES RELATING TO DATA QUALITY 1. Member States shall provide that personal data must be: (a) processed fairly and lawfully; (b) collected for specified, explicit and legitimate purposes and not further processed in a way incompatible with those purposes. [...] (c) adequate, relevant and not excessive in relation to the purposes for which they are collected and/or further processed; (d) accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that data which are inaccurate or incomplete, having regard to the purposes for which they were collected or for which they are further processed, are erased or rectified; (e) kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the data were collected or for which they are further processed. [...] | DATA INTEGRITY Consistent with the Principles, personal information must be relevant for the purposes for which it is to be used. An organization may not process personal information in a way that is incompatible with the purposes for which it has been collected or subsequently authorized by the individual. To the extent necessary for those purposes, an organization should take reasonable steps to ensure that data is reliable for its intended use, accurate, complete, and current. ACCESS Individuals must have access to personal information about them that an organization holds and be able to correct, amend, or delete that information where it is inaccurate, [...] |

¹⁵ Bernsdorff, in: Meyer, Charta der Grundrechte, Art. 8 Rn. 22.

¹⁶ Compare ECtHR, S. and Marper v. UK, no. 30562/04 and 30566/04, para. 103; Gardel v. France, no. 16428/05, para. 62.

¹⁷ Available at:

<http://www.oecd.org/internet/ieconomy/oecdguidelinesontheprivacyandtransborderflowsofpersonaldata.htm#part2>.

¹⁸ Available at: <http://conventions.coe.int/Treaty/en/Treaties/html/108.htm>.

b) Result of Comparison

The SHD mentions data quality requirements. However, crucial elements like “fairness” and “lawfulness” are missing. Since the element of “adequacy” is not mentioned in SH, there is no starting-point for conducting the proportionality test which is crucial in European data protection legislation.¹⁹

At a first glance the important minimum standard of purpose limitation is contained in the SHD. Nevertheless, the standard is formulated more generously. The SHD does not require the purpose to be “explicit”, “specified” or “legitimate”. This leads to the assumption that the principle can be easily circumvented. As the further elements (incompatibility; accuracy; completeness; currentness) refer to the defined purpose, the formulation of a broad purpose paves the way for various forms of processing. With regard to such broad definition of the purpose it is not unlikely that the data are regarded as relevant, necessary, compatible and current for various different purposes.

Concerning the concept of data minimization severe doubts arise if the SHD adheres to this principle. The SHD does not explicitly lay down that data must be “not excessive”. Additionally, the SHD lacks the clear order to retain data in a form which permits identification of data subjects only as long as it is necessary for the purposes.

All in all it can be observed that the SHD is differing in essential points from European data protection standards. Important minimum standards (fairness, lawfulness, adequacy, explicit purpose limitation) resulting from Directive 95/46, Article 7, 8 CFR and Article 8 ECHR are not applied at all or applied in a less stringent way.

2. Legitimate Processing

a) General Remarks

EU law prohibits data processing, unless there is an explicit allowance. This principle is – next to the data quality principles – the second main limitation on data usage. The general approach was already established in the ECHR. According to Article 8 (2) ECHR the basic requirement for the justification of an interference with the right of private and family life is the existence of a legal basis. Similarly, Article 8 CFR requires permission for every form of data processing operation as well. Directive 95/46 implements the principle by explicitly listing in Article 7 exceptional circumstances in which data processing is not prohibited.

The most relevant condition that makes data processing legitimate is the consent of the data subject. Additionally, the list contains five more reasons that can be applied for arguing that the processing operation is in conformity with data protection law. It is noteworthy that every option contains the word “necessary”. This leaves open the possibility to interpret the exceptions narrowly, which is in line with the general approach in EU law to which exceptions should not be interpreted too extensively.

¹⁹ Compare Article 29 Data Protection Working Party, 536/14/EN, available at: http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp211_en.pdf.

The SH does not know such a general limitation. Instead processing depends only on the application of the notice and choice principles. First, it is required to inform data subjects about the purposes for which data are collected and it is required to give certain additional information. Secondly, the choice principle necessitates the possibility to “opt out” (equivalent to the “right to object” in Article 14 of Directive 95/46) from data processing. But this possibility is limited to two specific situations, which are (a) disclosure to a third party and (b) incompatible usage. In consequence, most processing operations can take place without having to consider strict processing rules.

| Directive 95/46 | Safe Harbor |
|--|---|
| <p>Article 7, CRITERIA FOR MAKING DATA PROCESSING LEGITIMATE</p> <p>Member States shall provide that personal data may be processed only if:</p> <p>(a) the data subject has unambiguously given his consent; or</p> <p>(b) processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract; or</p> <p>(c) processing is necessary for compliance with a legal obligation to which the controller is subject; or</p> <p>(d) processing is necessary in order to protect the vital interests of the data subject; or</p> <p>(e) processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller or in a third party to whom the data are disclosed; or</p> <p>(f) processing is necessary for the purposes of the legitimate interests pursued by the controller or by the third party or parties to whom the data are disclosed, except where such interests are overridden by the interests for fundamental rights and freedoms of the data subject which require protection under Article 1 (1).</p> | <p>NOTICE</p> <p>An organization must inform individuals about the purposes for which it collects and uses information about them, how to contact the organization with any inquiries or complaints, the types of third parties to which it discloses the information, and the choices and means the organization offers individuals for limiting its use and disclosure.</p> <p>This notice must be provided in clear and conspicuous language when individuals are first asked to provide personal information to the organization or as soon thereafter as is practicable, but in any event before the organization uses such information for a purpose other than that for which it was originally collected or processed by the transferring organization or discloses it for the first time to a third party</p> <p>CHOICE</p> <p>An organization must offer individuals the opportunity to choose (opt out) whether their personal information is (a) to be disclosed to a third party or (b) to be used for a purpose that is incompatible with the purpose(s) for which it was originally collected or subsequently authorized by the individual.</p> <p>Individuals must be provided with clear and conspicuous, readily available, and affordable mechanisms to exercise choice.</p> |

b) Result of Comparison

The SHD follows a general processing approach which differs in essential points from EU data protection rules. In the EU processing of personal data is prohibited unless one of the explicitly listed exemptions applies.²⁰ Under SH, it is exactly the opposite. When applying the notice and choice principle, the general prohibition to process personal data is replaced by a general permission.

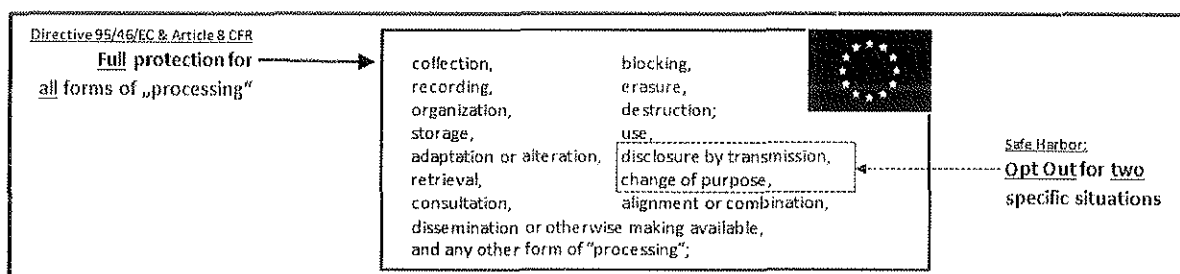
²⁰ Compare Boehm/Cole, Data Retention after the Judgement of the Court of Justice of the European Union, p. 49.

Analyzing the two principles in detail, doubts regarding the effectiveness of the protection occur. The information principle specifies the moment at which the US organization is obliged to inform the data subject. It says that the information must be provided when “individuals are first asked to provide personal information to the organization or as soon thereafter as is practicable”. These options leave considerable space for misuse. The US organization does not ask individuals to provide personal information to them. Instead, it imports data that was provided to them by an organization in the EU.

This strange construction in the SHD at least leaves open the possibility that US organizations delay the application of the information principle and by doing so weaken the data subjects’ rights.

Only if the receiving organization in the US “uses the information for a purpose other than that for which it was originally collected or processed by the transferring organization or discloses it for the first time to a third party”, the SHD leaves no space for delaying the necessary information. In that case the organization in the US clearly has to notify the data subject before the mentioned actions are carried out. Nevertheless, this stricter obligation can also be circumvented if already the transferring organization formulates a very broad purpose²¹ or if the notification requirement is overridden by US law. In consequence the information principle as one basic requirement for lawful data processing has considerable disadvantages compared to the standards guaranteed in the EU.

The structure of the second main principle, the choice principle, brings up further questions regarding the effectiveness of data protection in the US. It requires US organizations to offer data subjects the opportunity to “opt out” of specific processing operations. The option to opt out is an equivalent to the “right to object” in Article 14 of the Directive. It is applicable in only two situations, which are “usage for another purpose” or “disclosure to a third party”. These situations can, however, be restricted by US law. Every other processing operation can be conducted by the organization. Consequently, the data subject has quite often no influence on the handling of its personal data.



Furthermore, the opt-out-method has next to its limited application another structural shortcoming. The opportunity to opt out must be “provided with clear and conspicuous, readily available, and affordable mechanisms to exercise choice”. However, the determination that the data subject did not choose to opt out (when it comes to a change of purpose or disclosure to a third party) does not necessarily mean that it gave its consent to the processing operation. It is for example not unlikely that the data subject missed the option. This especially happens when a data subject faces a huge amount of information. Besides, it

²¹ Compare for instance facebook, statement of rights and responsibilities, legal terms, para 17, available at: <https://www.facebook.com/legal/terms>.

is doubtful if the option to opt-out is similar to giving consent “unambiguously”, which is required by Directive 95/46. While not opting-out means that a person behaves in a passive way, the approach in the Directive is based on activity by a person. From this observation one can conclude that SHD relies on a mechanism that at least cannot be regarded completely useful and effective for enforcing data protection standards. Against the background of this, the question arises why the application of the opt-out-method is limited to only a part of possible processing operations.

All things considered the protection of SH appears considerably lower than the minimal standards of Directive 95/46, Article 8 CFR (“data must be processed ... on the basis of the consent ... or some other legitimate basis laid down by law”) and even the OECD guidelines (see “Use Limitation Principle”).

3. Onward Transfer

a) General Remarks

Under Directive 95/46 the transfer of data respectively the “disclosure by transmission” constitutes a form of processing (Article 2 (b)). Therefore, the general limitations applicable to any “processing operation” apply. Transfers must be allowed under Articles 7 or 8 and the processing operation must fulfill the requirements of Article 6. Transfers outside of the area that is governed by Directive 95/46 (countries that are not members of the EU/EEA) fall under the additional limitations of Articles 25 and 26.

SH does not foresee any limitations on onward transfer other than “notice and choice”, which effectively means that data subjects must have an option to “opt out” of an onward transfer. Moreover, these principles can be overridden by US law (see above). Only if the recipient acts as an “agent” (“processor”), an adequate level of protection has to be granted. In all other cases the recipient of the data is not required to provide any form of an “adequate protection”.

| Directive 95/46 | Safe Harbor |
|---|--|
| <p>Article 25, TRANSFER OF PERSONAL DATA TO THIRD COUNTRIES</p> <p>The Member States shall provide that the transfer to a third country of personal data which are undergoing processing or are intended for processing after transfer may take place only if, without prejudice to compliance with the national provisions adopted pursuant to the other provisions of this Directive, the third country in question ensures an adequate level of protection. [...]</p> <p>Article 26 Derogations</p> <p>1. By way of derogation from Article 25 and save where otherwise provided by domestic law governing particular cases, Member States shall provide that a transfer or a set of transfers of personal data to a third country which does not ensure an adequate level of protection within the meaning of</p> | <p>ONWARD TRANSFER</p> <p>To disclose information to a third party, organizations must apply the Notice and Choice Principles.</p> <p><i>[The following section on “agents” refers to “processors” as defined in Article 2(e) of Directive 95/46/EC]</i></p> <p>Where an organization wishes to transfer information to a third party that is acting as an agent, as described in the endnote, it may do so if it first either ascertains that the third party subscribes to the Principles or is subject to the Directive or another adequacy finding or enters into a written agreement with such third party requiring that the third party provide at least the same level of privacy protection as is required by the relevant Principles.</p> <p>If the organization complies with these requirements, it shall</p> |

| | |
|--|--|
| <p>Article 25 (2) may take place on condition that:</p> <p>(a) the data subject has given his consent unambiguously to the proposed transfer; or</p> <p>(b) the transfer is necessary for the performance of a contract between the data subject and the controller or the implementation of precontractual measures taken in response to the data subject's request; or</p> <p>(c) the transfer is necessary for the conclusion or performance of a contract concluded in the interest of the data subject between the controller and a third party; or</p> <p>(d) the transfer is necessary or legally required on important public interest grounds, or for the establishment, exercise or defence of legal claims; or</p> <p>(e) the transfer is necessary in order to protect the vital interests of the data subject; or</p> <p>(f) the transfer is made from a register which according to laws or regulations is intended to provide information to the public and which is open to consultation either by the public in general or by any person who can demonstrate legitimate interest, to the extent that the conditions laid down in law for consultation are fulfilled in the particular case. [...]</p> | <p>not be held responsible (unless the organization agrees otherwise) when a third party to which it transfers such information processes it in a way contrary to any restrictions or representations, unless the organization knew or should have known the third party would process it in such a contrary way and the organization has not taken reasonable steps to prevent or stop such processing.</p> |
|--|--|

b) Result of Comparison

Both regulations follow the approach that data generally may not leave a sphere of “adequate protection”. Under SH this is realized by obliging US organizations to apply the notice and choice principles. Theoretically, the data subject should on the basis of these principles be in the position to prevent the onward transfer if it does not want it to happen. This could lead to the assumption that the protection standard is higher than in the EU, where a general allowance for transfers to countries with an adequate level of protection exists. In the SH framework it appears that the data subject can influence the handling of its data in every single case.

But practically, the shortcomings of the principles become clear in the situation of onward transfers. Especially the opt-out-method has a negative effect on data protection standards in these situations (see above). With regard to the right to opt out it is also unclear, whether it must be applied in a situation where a data subject has “agreed” to forwarding of data through signing terms, privacy policies or other kinds of consent forms far before it actually comes to the transfer. It is questionable if such forms constitute an “informed, specific and unambiguous consent”.

Besides, it must be observed that there are many exceptions to the SH. For example, US laws may allow or require to forward data to entities that do not provide for any guarantee (see exceptions above). All in all there is a wide scope of situations where onward transfer may be allowed.

4. Summary Substantive Law Guarantees

At a first glance the SHD contains most of the important ideas and principles that are laid down in Directive 95/46 in order to grant sufficient material protection for data subjects. But a closer look reveals

several weaknesses that raise the question if the principles are principally adequate to European standards.

The comparison of the provisions regulating data quality led to the conclusion that the requirements are implemented just superficially in the SHD. Important elements that can be found in Directive 95/46 were not transposed into the SHD. The lack of those elements results in missing crucial minimum standards such as the possibility to conduct a proportionality test, the strict purpose limitation principle and the idea of data minimization.

The SHD also follows a general approach on the question of legitimacy of processing that is disadvantageous for individuals compared to the European standards. There is no general prohibition of data processing operations but only the obligation to apply the notice and choice principles. These two basic principles suffer from structural as well as practical problems.

The structural and practical problems within the principles also have an impact on the possibility to transfer data to third parties. Additionally, exceptions and vague terms in the SHD weaken an effective protection from the onward transfer of data.

Considering these observations, one can conclude that the material protection granted by the SHD does not even come close to the level of protection Directive 94/46 offers to data subjects.

III. RIGHTS OF DATA SUBJECTS

1. Right to Access/Erasure/Rectification/Blocking

a) General Remarks

The right of an individual to access personal data is laid down in Article 12 of Directive 95/46. The same article also refers to the right to erasure, rectification and blocking of data that does not comply with the requirements of Directive 95/46. These rights are further specified in the national laws of the member states, for instance, with regard to the duration and costs of access.

Under SH the rights to access, correction, amendment and deletion are mentioned in Annexes I and II (FAQ 8). Annex I refers to these rights while Annex II limits the access right established in Annex I to a great extent.

According to Annex II (FAQ 8), the right to access is “subject to the principle of proportionality or reasonableness” or may be limited to data that is “readily available and inexpensive to provide” if “the information requested is not sensitive or not used for decisions that will significantly affect the individual”. Equally “confidential commercial information” is excluded, as well as cases where access is “likely to interfere with the safeguarding of important countervailing public interests”. The companies may also charge costs of the access that are “not excessive” which (according to the FAQs) “may be useful in discouraging repetitive and vexatious requests”. The time-limit to provide an answer is defined as “without excessive delay and within a reasonable time period”.

In addition, the rights to deletion, correction and amendment are limited to data that is “inaccurate”. In contrast to EU law, the rights do not refer to data that is processed illegally or in violation of the SH rules.²² As long as the content of the information is correct, there is thus no possibility of obtaining a deletion, correction and amendment of the data. This clearly contradicts established EU data protection principles.²³ Moreover, there is no possibility to obtain access, erasure, rectification or blocking of data that is accessed by US surveillance programs or transferred to others due to other legal obligations mentioned above.²⁴

| Directive 95/46 | Safe Harbor |
|--|---|
| <p>Article 12, Right of access</p> <p>Member States shall guarantee every data subject the right to obtain from the controller:</p> <p>(a) without constraint at reasonable intervals and without excessive delay or expense:</p> <ul style="list-style-type: none"> - confirmation as to whether or not data relating to him are being processed and information at least as to the purposes of the processing, the categories of data concerned, and the recipients or categories of recipients to whom the data are disclosed, - communication to him in an intelligible form of the data undergoing processing and of any available information as to their source, - knowledge of the logic involved in any automatic processing of data concerning him at least in the case of the automated decisions referred to in Article 15 (1); <p>(b) as appropriate the rectification, erasure or blocking of data the processing of which does not comply with the provisions of this Directive, in particular because of the incomplete or inaccurate nature of the data;</p> <p>(c) notification to third parties to whom the data have been disclosed of any rectification, erasure or blocking carried out in compliance with (b), unless this proves impossible or involves a disproportionate effort.</p> | <p>ACCESS</p> <p>Individuals must have access to personal information about them that an organization holds and be able to correct, amend, or delete that information where it is inaccurate, except where the burden or expense of providing access would be disproportionate to the risks to the individual's privacy in the case in question, or where the rights of persons other than the individual would be violated.</p> <p><i>See “FAQ 8 – Access” of Annex II of the Safe Harbor Decision for numerous vague limitations and exceptions.</i></p> |

²² Compare Annex I of the SHD.

²³ Compare, for instance, Article 12 of Directive 95/46; Compare Boehm/Cole, Data Retention after the Judgement of the Court of Justice of the European Union, p. 28 et seq.

²⁴ Compare Communication of the Commission on the functioning of SH, p. 16 et seq., in particular para 7.2; for earlier assessments compare: Impact Assessment Study prepared for the European Commission in 2008 by the Centre de Recherche Informatique et Droit ('CRID') of the University of Namur; Commission Staff Working Paper “The application of Commission Decision 520/2000/EC of 26 July 2000 pursuant to Directive 95/46 of the European Parliament and of the Council on the adequate protection of personal data provided by the Safe Harbour Privacy Principles and related FAQs issued by the US Department of Commerce”, SEC (2002) 196, 13.12.2002 and Commission Staff Working Paper “The implementation of Commission Decision 520/2000/EC on the adequate protection of personal data provided by the Safe Harbour Privacy Principles and related FAQs issued by the US Department of Commerce”, SEC (2004) 1323, 20.10.2004.

b) Result of Comparison

The rights of access, correction, amendment and deletion in SH are formulated similar to Article 12 of Directive 95/46, but they are lacking further determination as currently provided for in the national laws of the member states for the provisions of the Directive. Only the access right is specified in Annex II (FAQ 8). This specification provides for a wide variety of exceptions and limitations to the right of access. This is aggravated by the fact that the existing guidelines on the application of the access right in Annex II are rather vague and difficult to enforce.

It is also worth noting that the rights to have data deleted, corrected or amended are limited in SH and can only be exercised in relation to "inaccurate" data. This clearly limits the possibility of the individual to remedy data that may be illegally processed or processed against the rules of SH.

2. Information Duties

a) General Remarks

The regulation of information duties of SH and Directive 95/46 appear to be similar in essential points.

| Directive 95/46 | Safe Harbor |
|---|---|
| <p>Article 10, INFORMATION TO BE GIVEN TO THE DATA SUBJECT</p> <p>Information in cases of collection of data from the data subject</p> <p>Member States shall provide that the controller or his representative must provide a data subject from whom data relating to himself are collected with at least the following information, except where he already has it:</p> <p>(a) the identity of the controller and of his representative, if any;</p> <p>(b) the purposes of the processing for which the data are intended;</p> <p>(c) any further information such as</p> <ul style="list-style-type: none"> - the recipients or categories of recipients of the data, - whether replies to the questions are obligatory or voluntary, as well as the possible consequences of failure to reply, - the existence of the right of access to and the right to rectify the data concerning him in so far as such further information is necessary, having regard to the specific circumstances in which the data are collected, to guarantee fair processing in respect of the data subject. <p>Article 11</p> <p>Information where the data have not been obtained from the data subject</p> <p>1. Where the data have not been obtained from the data subject, Member States shall provide that the controller or his representative must at the time of undertaking the recording</p> | <p>NOTICE</p> <p>An organization must inform individuals about the purposes for which it collects and uses information about them, how to contact the organization with any inquiries or complaints, the types of third parties to which it discloses the information, and the choices and means the organization offers individuals for limiting its use and disclosure.</p> <p>This notice must be provided in clear and conspicuous language when individuals are first asked to provide personal information to the organization or as soon thereafter as is practicable, but in any event before the organization uses such information for a purpose other than that for which it was originally collected or processed by the transferring organization or discloses it for the first time to a third party (1).</p> <p>(1) It is not necessary to provide notice or choice when disclosure is made to a third party that is acting as an agent to perform task(s) on behalf of and under the instructions of the organization. The Onward Transfer Principle, on the other hand, does apply to such disclosures.</p> |

| | |
|--|--|
| <p>of personal data or if a disclosure to a third party is envisaged, no later than the time when the data are first disclosed provide the data subject with at least the following information, except where he already has it:</p> <p>(a) the identity of the controller and of his representative, if any;</p> <p>(b) the purposes of the processing;</p> <p>(c) any further information such as</p> <ul style="list-style-type: none"> - the categories of data concerned, - the recipients or categories of recipients, - the existence of the right of access to and the right to rectify the data concerning him in so far as such further information is necessary, having regard to the specific circumstances in which the data are processed, to guarantee fair processing in respect of the data subject. <p>2. Paragraph 1 shall not apply where, in particular for processing for statistical purposes or for the purposes of historical or scientific research,[...]</p> | |
|--|--|

b) Result of Comparison

Directive 95/46 requires slightly more detailed information to guarantee a “fair processing” than the SH. However, the information that theoretically should be given to the data subject is similar in both instruments and can be regarded as providing an adequate level of protection. The Commission however, constituted in a recent report on the practical functioning of SH after the PRISM revelations that there are situations in which individuals “may not be made aware by [...] companies that their data may be subject to access” by third parties.²⁵ This leads to a practical enforcement problem, which can also influence the exercise of the access rights and therefore needs to be considered when comparing the two instruments. If individuals are not aware of the fact that their data is transferred to third parties, they may refrain from exercising their access right.

3. Summary Rights of the Data Subject

Comparing the rights of access, deletion, correction and amendment leads to the following conclusions: The right of access under SH in Annex I is formulated in a similar way as in Directive 95/46. This similarity however ends when looking at the wide exceptions provided for in Annex II of the SH. On the one hand, there are several possibilities to restrict the access right, on the other hand the conditions for access are not defined in a way to enable persons concerned to understand the necessary legal details to enforce the access right. In the EU, such details are included in the national laws of the member states.

In addition to the restricted access right, the rights of deletion, correction and amendment are limited to cases in which the data is “inaccurate”. SH lacks a remedy in cases where data is simply illegally processed but not inaccurate. Dispute resolution bodies may require organizations to remove or delete data as a “sanction” but the data subject has no subjective right to the removal.

²⁵ Compare Communication of the Commission on the functioning of SH, p. 16 et seq., in particular para 7.3.

When comparing the right to information, there is no fundamental difference between the right of Directive 95/46 and the information that needs to be provided according to the SH rules. However, there seems to be rather a practical enforcement problem that partly leads to the situation that individuals “may not be made aware by those companies that their data may be subject to access” by third parties.²⁶ In consequence, individuals concerned may not be informed about all details regarding the processing of their data and may refrain from exercising their access rights simply because they are not aware of the extent to which their data is used.

IV. ENFORCEMENT

1. Remedies

a) General Remarks

One of the most important issues with regard to the effective enforcement of fundamental rights relates to the possibility to claim a remedy before independent courts in cases of violations of the respective rights. This right is entailed in the ECHR, in the CFR and concretized in Article 22 of Directive 95/46 that guarantees a right for judicial remedies before a court for violations of the right to data protection.²⁷ One essential requirement to comply with this right is that the remedies are effective meaning that the remedy must be “sufficiently certain not only in theory but also in practice and must be effective in practice as well as in law”.²⁸ The remedies usually refer to proceedings to obtain injunctive relief and/or damages. The concrete application of this right is left to the respective legal system of each member state.

The SHD lists in Annex IV examples for cases in which damages may be claimed in US law, but does not provide for any independent cause of action due to a violation of the right to data protection. As the right to data protection is not known in the US jurisdiction, an individual concerned would have to refer to the existing civil law claims in US law and to the more broad application of the right to privacy in US case law. Annex IV of the SHD particularly refers to cases of fraudulent misrepresentation of facts, opinions, intentions or law “for the purpose of inducing another to act or to refrain from action in reliance upon it”²⁹, but rarely lists cases in which damages are awarded for privacy violations. Moreover, as mentioned above, some of the laws that interfere with data protection rights of individuals do not

²⁶ Compare Communication of the Commission on the functioning of SH p. 16 et seq., in particular para 7.3.

²⁷ Article 13 ECHR in connection with another right and Article 47 CFR.

²⁸ Compare Guide to good practice in respect of domestic remedies, adopted by the Committee of Ministers of the Council of Europe on 18 September 2013, p. 12, which refers to the cases: *McFarlane v. Ireland*, App. No. 31333/06, 10 September 2010, paragraph 114; *Riccardi Pizzati v. Italy*, App. No. 62361/00, Grand Chamber judgment of 29 March 2006, paragraph 38; *El-Masri v. “the former Yugoslav Republic of Macedonia”*, App. No. 39630/09, 13 December 2012, paragraph 255; *Kudła v. Poland*, App. No. 30210/96, judgment of 26 October 2000, paragraph 152.

²⁹ Compare Annex IV A of the SHD.

allow for the protection of EU citizens. Therefore it seems to be difficult to enact a civil law claim in US law for EU citizens.

A more concrete dispute resolution procedure is established in Annex II of the SH. FAQ 11 refers to alternative dispute resolution bodies that should handle claims of EU citizens in the first place. These dispute resolution bodies can refer a case to the FTC. The bodies will examine whether a SH certified company violates section 5 of the Federal Trade Commission Act (FTC Act) which prohibits “unfair or deceptive acts or practices in or affecting commerce.” Section 5 of the FTC Act applies “to all persons engaged in commerce, including banks”. The main dispute resolution bodies in this field are TRUSTe and BBB (Better Business Bureaus).

Alternatively, companies can choose to collaborate with the EU Data Protection Panel which is competent to deal with SH claims in the framework of human resources data. This panel is composed of representatives of EU data protection authorities and very rarely used.³⁰

| | |
|--|---|
| Directive 95/46 | Safe Harbor |
| <p>Article 22 - Remedies</p> <p>Without prejudice to any administrative remedy for which provision may be made, inter alia before the supervisory authority referred to in Article 28, prior to referral to the judicial authority, Member States shall provide for the right of every person to a judicial remedy for any breach of the rights guaranteed him by the national law applicable to the processing in question.</p> <p>Article 23 - Liability</p> <p>1. Member States shall provide that any person who has suffered damage as a result of an unlawful processing operation or of any act incompatible with the national provisions adopted pursuant to this Directive is entitled to receive compensation from the controller for the damage suffered. [...]</p> | <p>ANNEX IV Damages for Breaches of Privacy, Legal Authorizations and Mergers and Takeovers in U.S. Law</p> <p>Failure to comply with the safe harbor principles could give rise to a number of private claims depending on the relevant circumstances</p> <p><i>(Examples, see Annex IV of the SHD for details)</i></p> <p>Annex II, FAQ No 11, Dispute Resolution and Enforcement</p> <p>FTC Action</p> <p>The FTC has committed to reviewing on a priority basis referrals received from privacy self-regulatory organizations, such as BBBOnline and TRUSTe, and EU Member States alleging non-compliance with the Safe Harbor Principles to determine whether Section 5 of the FTC Act prohibiting unfair or deceptive acts or practices in commerce has been violated.</p> <p><i>(Examples, see Annex II of the SHD for details)</i></p> |

b) Result of Comparison

While Directive 95/46 establishes a basis for effective remedies in national laws, mainly in form of injunctive relieve and damages, SH refers to the existing US civil law claims and establishes an Alternative Dispute Resolution (ADR) mechanism with links to the FTC. The FTC, however, is restricted to examine possible violations of section 5 of the FTC Act. It does not have the legal authority to remedy cases beyond the scope of application of this section. It is therefore not possible to obtain a remedy in a case

³⁰ Compare Communication of the Commission on the functioning of SH, p. 13, in particular para 5.2.

which does not refer to unfair or deceptive acts or practices in commerce through the FTC. This concerns violations of the SH principles by, for instance, public authorities that may violate SH principles by massively accessing SH data.

In addition to this legal restraint, the ADR mechanism is not very effective in practice. Therefore the Commission, in its report on the functioning of SH, criticizes that the effectiveness of this mechanism is not proven.³¹ The example of TRUSTe is given:

“[...] that reported that it received 881 requests in 2010, but that only three of them were considered admissible, and grounded, and led to the company concerned being required to change its privacy policy and website. In 2011, the number of complaints was 879, and in one case the company was required to change its privacy policy”.³²

The restriction of investigation powers of the FTC to Section 5 of the FTC Act and the practical difficulties in enforcing violations through the ADR bodies lead to the assumption that remedies are not effective in practice in SH. This contradicts the EU understanding of an effective remedy that must be certain not only in theory but also in practice. In addition, these ADR bodies seem to “lack appropriate means to remedy cases of failure to comply with the [SH] principles”.³³ In consequence, there are important shortcomings regarding not only the enforcement in practice, but also in theory concerning the means to remedy a possible violation of SH principles.

In addition to these figures, most of the ADR providers charge a considerable fee for consumers for filling a complaint. This contradicts the guarantees of SH which requires an affordable recourse mechanism.³⁴

2. Notification/Prior Checking/Publicizing

a) General Remarks

Directive 95/46 requires mechanisms which guarantee control over data processing activities. Chapter IX of Directive 95/46 obliges data controllers to notify the supervisory authority or the data controller must appoint a data protection officer (currently only in Germany). Data processing presenting a specific risk to the rights of the individuals is subject to prior checking.

SH follows a completely different approach and does not include duties of general overview or checking. Instead the companies subscribing to SH apply a “self-certification” method, which means in practice that the oversight work carried out by the supervisory authority (or data protection official) in the EU is done by the organization itself in the US.

³¹ Compare Communication of the Commission on the functioning of SH, p. 14, in particular para 6.1 and also Communication of the Commission on Rebuilding Trust in EU-US Data Flows, COM(2013) 846 final.

³² Communication of the Commission on the functioning of SH, pp. 14-15, in particular para 6.1, footnote 46.

³³ Ibid, p. 10, in particular para 5.

³⁴ Ibid, p. 15, in particular para 6.1.

| Directive 95/46 | Safe Harbor |
|---|--|
| <p>NOTIFICATION</p> <p>Article 18 - Obligation to notify the supervisory authority</p> <p>1. Member States shall provide that the controller or his representative, if any, must notify the supervisory authority referred to in Article 28 before carrying out any wholly or partly automatic processing operation or set of such operations intended to serve a single purpose or several related purposes. [...]</p> <p>Article 19 - Contents of notification</p> <p>1. Member States shall specify the information to be given in the notification. It shall include at least: [...]</p> <p>Article 20 - Prior checking</p> <p>1. Member States shall determine the processing operations likely to present specific risks to the rights and freedoms of data subjects and shall check that these processing operations are examined prior to the start thereof. [...]</p> <p>Article 21 - Publicizing of processing operations</p> <p>1. Member States shall take measures to ensure that processing operations are publicized. [...]</p> | <p>FAQ 6 - Self-Certification</p> <p>Q: How does an organization self-certify that it adheres to the Safe Harbor Principles?</p> <p>A: Safe harbor benefits are assured from the date on which an organization self-certifies to the Department of Commerce (or its designee) its adherence to the Principles in accordance with the guidance set forth below.</p> <p>To self-certify for the safe harbor, organizations can provide to the Department of Commerce (or its designee) a letter, signed by a corporate officer on behalf of the organization that is joining the safe harbor, that contains at least the following information:</p> <p>1. name of organization, mailing address, e-mail address, telephone and fax numbers; 2. description of the activities of the organization with respect to personal information received from the EU; and 3. description of the organization's privacy policy for such personal information, including: (a) where the privacy policy is available for viewing by the public, (b) its effective date of implementation, (c) a contact office for the handling of complaints, access requests, and any other issues arising under the safe harbor, (d) the specific statutory body that has jurisdiction to hear any claims against the organization regarding possible unfair or deceptive practices and violations of laws or regulations governing privacy (and that is listed in the annex to the Principles), (e) name of any privacy programs in which the organization [...]</p> <p>Q: How do organizations provide follow up procedures for verifying that the attestations and assertions they make about their safe harbor privacy practices are true and those privacy practices have been implemented as represented and in accordance with the Safe Harbor Principles?</p> <p>A: To meet the verification requirements of the Enforcement Principle, an organization may verify such attestations and assertions either through self-assessment or outside compliance reviews. [...]</p> |

b) Result of Comparison

There is a fundamental difference when it comes to the control of data processing activities by data controller between the EU and the SH system. The self-certification mechanism of SH does not require any external control or review that ensures compliance with the SH principles. The self-certification is completed through a letter to the Department of Commerce with basic information about the organization. Follow up procedures can be equally carried out by the organization itself. There is also "no full evaluation of the actual practice in self-certified companies".³⁵ The Commission therefore requires "an active follow up by the Department of Commerce on effective incorporation of the Safe Harbour

³⁵ Compare Communication of the Commission on the functioning of SH, p. 8, in particular para 4.

principles [...].”³⁶ So far, a self-certified company comes only under scrutiny after an individual uses the enforcement mechanisms that are available to him.³⁷

The lack of notification, prior checking and external control of the SH principles is hardly in compliance with the requirements of EU data protection rights. The Court of Justice regularly requires independent control of data processing activities to assure that basic rights are respected.³⁸ Refraining from one of the essential data protection requirements by accepting the SH self-certifying mechanism clearly interferes with the guarantees of Article 7 and 8 CFR and 8 ECHR and cannot be regarded as providing an adequate level of protection anymore.

3. Supervisory Authority/Enforcement

a) General Remarks

Connected to the notification and prior checking requirement is the exercise of independent control.³⁹ Article 28 of Directive 95/46 (together with the general principles of EU law, national laws and Article 8 III CFR) provides for the establishment of independent supervisory authorities in each member state. They are equipped with enforcement and investigations powers and must process complaints filed by data subjects. The supervisory authorities are described by the Court of Justice as “the guardians of [...] fundamental rights and freedoms, and their existence in the Member States is considered, as is stated in the 62nd recital in the preamble to Directive 95/46, as an essential component of the protection of individuals with regard to the processing of personal data.”⁴⁰ They must be completely independent meaning that they must be free from any external influence. The mere risk that such influence could be exercised over the decisions of the supervisory authorities is “enough to hinder the latter authorities’ independent performance of their tasks”.⁴¹

As already seen above, SH only foresees the FTC as investigative authority, while “dispute resolution bodies” can only decide over complaints but lack power to investigate the facts. The ADR bodies are chosen and paid by the SH organization and therefore not independent in the sense of EU data protection law.

³⁶ Compare Communication of the Commission on the functioning of SH, p. 8, in particular para 4.

³⁷ According to the communication of the Commission on the functioning of SH, the FTC initiated 10 enforcement actions against self-certified SH companies until 2013, compare p. 10.

³⁸ Compare: C-518/07, *Commission v. Germany* of 9 March 2010 and case C-614/10, *European Commission v. Republic of Austria* of 16 Oct. 2012, Case C-288/12, *European Commission v Hungary* of 8 April 2014.

³⁹ Compare: C-518/07, *Commission v. Germany* of 9 March 2010 and case C-614/10, *European Commission v. Republic of Austria* of 16 Oct. 2012, Case C-288/12, *European Commission v Hungary* of 8 April 2014.

⁴⁰ C-518/07, *Commission v. Germany* of 9 March 2010, para 23.

⁴¹ C-518/07, *Commission v. Germany* of 9 March 2010, para 36.

Data subjects may also direct their requests to the FTC, but the FTC is not obliged to investigate consumer complaints.⁴² According to the Communication of the Commission on the functioning of SH, it seems that the FTC has so far only reviewed a few complaints of EU data protection authorities, but no complaints filed by EU data subjects.⁴³ The few enforcement actions taken by the FTC (10 until 2013) were also mainly based on interventions from EU bodies, or referred to broader violations of section 5 of the FTC Act in the privacy field.

| Directive 95/46 | Safe Harbor |
|---|--|
| Article 28, Supervisory authority 1. Each Member State shall provide that one or more public authorities are responsible for monitoring the application within its territory of the provisions adopted by the Member States pursuant to this Directive. [...] 3. Each authority shall in particular be endowed with: <ul style="list-style-type: none"> - investigative powers, such as powers of access to data forming the subject-matter of processing operations and powers to collect all the information necessary for the performance of its supervisory duties, - effective powers of intervention, such as, for example, that of delivering opinions before processing operations are carried out, in accordance with Article 20, and ensuring appropriate publication of such opinions, of ordering the blocking, erasure or destruction of data, of imposing a temporary or definitive ban on processing, of warning or admonishing the controller, or that of referring the matter to national parliaments or other political institutions, - the power to engage in legal proceedings where the national provisions adopted pursuant to this Directive have been violated or to bring these violations to the attention of the judicial authorities. Decisions by the supervisory authority which give rise to complaints may be appealed against through the courts. [...] | ENFORCEMENT Effective privacy protection must include mechanisms for assuring compliance with the Principles, recourse for individuals to whom the data relate affected by non-compliance with the Principles, and consequences for the organization when the Principles are not followed. At a minimum, such mechanisms must include <ul style="list-style-type: none"> (a) readily available and affordable independent recourse mechanisms by which each individual's complaints and disputes are investigated and resolved by reference to the Principles and damages awarded where the applicable law or private sector initiatives so provide; (b) follow up procedures for verifying that the attestations and assertions businesses make about their privacy practices are true and that privacy practices have been implemented as presented; and (c) obligations to remedy problems arising out of failure to comply with the Principles by organizations announcing their adherence to them and consequences for such organizations. [...] |

b) Result of Comparison

While Directive 95/46 as well as Article 8(3) CFR require a completely independent supervisory authority equipped with investigation and enforcement powers, the SH provides for the dispute resolution mechanism which shifts the control of the SH principles to private organizations that are chosen and paid by the SH companies. These organizations do not have investigative powers and cannot be regarded as independent within the meaning of EU law. Moreover, they do not exercise an active control over data processing activities of the SH companies; they only react to complaints of consumers. This concept is

⁴² Compare: A Brief Overview of the Federal Trade Commission's Investigative and Law Enforcement Authority: <http://www.ftc.gov/about-ftc/what-we-do/enforcement-authority> and <https://www.ftccomplaintassistant.gov/#crnt&panel1-1> that says: "The FTC cannot resolve individual complaints, but we can provide information about what next steps to take".

⁴³ Communication of the Commission on the functioning of SH, p. 11, para 5.1.

totally different from the EU understanding of independent control, which is in various cases a proactive control to prevent fundamental rights' violations before they arise.

There is also the possibility to refer a complaint to the FTC, which has however so far not investigated a complaint of an EU consumer.

4. Sanctions

a) General Remarks

Directive 95/46 requires Member States to lay down sanctions for breaches of the directive. The sanctions are set by each Member State and vary greatly (e.g. up to € 25.000 - or even imprisonment in certain cases - in Austria; up to € 100.000 in Ireland; up to € 300.000 or even higher in Germany).

The SHD establishes a stepwise sanction system. As a first step it is laying the task to sanction violations on "dispute resolution bodies". These can choose from sanctions that vary in their degree of severity. The SHD lists sanctions like "public findings of non-compliance", "requirements to delete data", "suspension or removal of a seal", "compensation for losses" or "injunctive orders". Failures to comply with these rulings must be notified not only to the Department of Commerce but also to the governmental body with applicable jurisdiction or to courts.

As a second step, violations can be indirectly sanctioned by the FTC through its authority in Section 5 of the FTC act. If the FTC concludes that Section 5 has been violated, it may "resolve the matter by seeking an administrative cease and desist order prohibiting the challenged practices or by filing a complaint in a federal district court, which if successful could result in a federal court order to the same effect" (FAQ 11). If the administrative or the federal orders are violated, the FTC may obtain civil penalties or pursue civil or criminal contempt.

A further step would be an action due to "persistent failure to comply with the principles". FAQ 11 explains this behavior more detailed. "Persistent failure to comply" may be actionable under the False Statements Act (18 U.S.C. § 1001) with up to five years of imprisonment.

| Directive 95/46/EC | Safe Harbor |
|---|--|
| <p>Article 24, SANCTIONS</p> <p>The Member States shall adopt suitable measures to ensure the full implementation of the provisions of this Directive and shall in particular lay down the sanctions to be imposed in case of infringement of the provisions adopted pursuant to this Directive.</p> | <p>ENFORCEMENT</p> <p>[...] Sanctions must be sufficiently rigorous to ensure compliance by organizations.</p> <p>FAQ 11: Remedies and Sanctions.</p> <p>The result of any remedies provided by the dispute resolution body should be that the effects of non-compliance are reversed or corrected by the organization, in so far as feasible, and that future processing by the organization will be in conformity with the Principles and, where appropriate, that processing of the personal data of the individual who has brought the complaint will cease.</p> |

| | |
|--|--|
| | Sanctions need to be rigorous enough to ensure compliance by the organization with the Principles. [...] Sanctions should include both publicity for findings of non-compliance and the requirement to delete data in certain circumstances. Other sanctions could include suspension and removal of a seal, compensation for individuals for losses incurred as a result of non-compliance and injunctive orders. [...] |
|--|--|

b) Result of Comparison

Both systems require sanctions. However, the “sanctions” provided for in the SHD at first step are mainly remedies. According to the 2013 annual report of the largest dispute resolution body (TRUSTe), companies are usually only required to change their policy, sanctions are not imposed.⁴⁴

Under the FTC act and the False Statements Act more severe actions can be initiated. The provisions are supposedly in conformity with the provisions in the Directive. Nevertheless, the system that is implemented is quite different. It is not only complicated but relies also in large parts on the participation of dispute resolution bodies and the concerned organizations.

In consequence, it seems doubtful that the FTC (or the Department of Commerce) initiates proceedings of its own accord. In practice, all but one of the enforcement actions so far led to “settlements” between the FTC and organizations that violated the SH; a fine on the respective organization was not imposed.⁴⁵

5. Summary Enforcement

Comparing the enforcement mechanisms of Directive 95/46 and the SH rules, doubts arise regarding the effective enforcement of remedies, sanctions and notification duties as well as the establishment of independent supervisory bodies within the SH framework.

With regard to effective remedies, it is doubtful whether the limited jurisdiction of the FTC and the ADR mechanism, which faces practical enforcement difficulties, can be classified as adequate according to the criteria mentioned in Article 25 (2) of Directive 95/46. The SH does not expressly establish a new cause of action for damages or an injunctive relief, contrary to the requirements of Directive 95/46. Instead Annex IV of the SHD only refers to the general US civil law and does not indicate that SH itself is enforceable. In addition to such legal uncertainties, individuals may also face practical difficulties when it comes to travel, costs and language barriers in case of civil law claims. The theoretical as well as the practical enforcement of remedies in the SH framework is thus very limited.

A comparison of the control mechanisms reveals further fundamental differences. While the control of data processing activities in the EU includes notification, prior checking and external control of such activities, the SH establishes a self-certifying mechanism which largely refrains from external control procedures. Dispute resolution bodies, for instance, are chosen by the organizations processing the data

⁴⁴ TRUSTe Transparency Report 2013, available at: <http://www.truste.com/window.php?url=http://download.truste.com/TVarsTf=3L0AXBJO-470>.

⁴⁵ Compare figure 1.

and can therefore not be regarded as independent within the meaning of EU law.⁴⁶ According to EU law, only independent control mechanisms can assure compliance with data protection and privacy rights. Thus, the concept of control over data processing activities in SH is contrary to the concept established by Directive 95/46 and Article 8 CFR.

In contrast to the ADR bodies, the FTC is an independent organization, which is equipped with investigative powers. Its investigations can lead to sanctions being imposed on the companies violating section 5 of the FTA Act. Sanctions are, however, very rare.⁴⁷ Moreover, the FTC is usually not actively reviewing and investigating the factual practices of companies. Further, complaints by individual data subjects are not investigated in practice. In summary, there are serious doubts on the SH adequacy finding with regard to enforcement. Criticism refers mainly to the non-effective enforcement of remedies and the self-controlling mechanism when it comes to oversight and control mechanisms over data processing activities within the SH framework. Therefore, the existing procedures do not satisfy the EU requirements with regard to enforcement.

Figure 1: registration settlements in context with SH (2014)

| Registration Settlements (2014) | | | |
|--|------------------|-------------------------------|--|
| 1 ExpatEdge Partners, LLC, FTC File No. 0923138 | November 9, 2009 | Certification Lapsed | settled: prohibition from further misrepresentations, no fine |
| 2 Onyx Graphics, Inc., FTC File No. 0923139 | November 9, 2009 | Certification Lapsed | settled: prohibition from further misrepresentations, no fine |
| 3 Progressive Gaitways LLC, FTC File No. 0923141 | November 9, 2009 | Certification Lapsed | settled: prohibition from further misrepresentations, no fine |
| 4 Collectify LLC, FTC File No. 0923142 | November 9, 2009 | Certification Lapsed | settled: prohibition from further misrepresentations, no fine |
| 5 World Innovators, Inc., FTC File No. 0923137 | January 12, 2010 | Certification Lapsed | settled: prohibition from further misrepresentations, no fine |
| 6 Directors Desk LLC, FTC File No. 0923140 | January 12, 2010 | Certification Lapsed | settled: prohibition from further misrepresentations, no fine |
| 7 Javian Karnani, and Balls of Kryptonite, LLC, Civ. No. 095276 | May 16, 2011 | Mainly: Online Fraud, SH: Not | settled: prohibition from further misrepresentations, \$ 500.000 |
| Material Settlements (2011-12) | | | |
| 8 Google Inc., FTC File No. 1023136 | March 30, 2011 | Sec. 5 FTC Act & SH | settled: no further misrepresentation, improvements, external |
| 9 Facebook, Inc., FTC File No. 0923184 | November 29, | Sec. 5 FTC Act & SH | settled: no further misrepresentation, improvements, external |
| 10 My Space, LLC, FTC File No. 1023058 | May 8, 2012 | Sec. 5 FTC Act & SH | settled: no further misrepresentation, external audits, no fine |
| Registration Settlements (2014) | | | |
| 11 American Apparel, Inc., FTC File No. 1423036 | June 25, 2014 | Certification Lapsed | settled: prohibition from further misrepresentations, no fine |
| 12 Apperian, Inc., FTC File No. 1423017 | June 25, 2014 | Certification Lapsed | settled: prohibition from further misrepresentations, no fine |
| 13 Atlanta Falcons Football, LLC, FTC File No. 1423018 | June 25, 2014 | Certification Lapsed | settled: prohibition from further misrepresentations, no fine |
| 14 Baker Tilly Virchow Krause, LLP, FTC File No. 1423019 | June 25, 2014 | Certification Lapsed | settled: prohibition from further misrepresentations, no fine |
| 15 BitTorrent, Inc., FTC File No. 1423020 | June 25, 2014 | Certification Lapsed | settled: prohibition from further misrepresentations, no fine |
| 16 Charles River Labs International, Inc., FTC File No. 1423022 | June 25, 2014 | Certification Lapsed | settled: prohibition from further misrepresentations, no fine |
| 17 DataMotion, Inc., FTC File No. 1423023 | June 25, 2014 | Certification Lapsed | settled: prohibition from further misrepresentations, no fine |
| 18 DDC Laboratories, Inc., FTC File No. 1423024 | June 25, 2014 | Certification Lapsed | settled: prohibition from further misrepresentations, no fine |
| 19 Fantage, Inc., FTC File No. 1423026 | June 25, 2014 | Certification Lapsed | settled: prohibition from further misrepresentations, no fine |
| 20 Level 3 Communications, LLC, FTC File No. 1423028 | June 25, 2014 | Certification Lapsed | settled: prohibition from further misrepresentations, no fine |
| 21 PBD Sports, Ltd. d/b/a Denver Broncos Football Club, FTC File No. | June 25, 2014 | Certification Lapsed | settled: prohibition from further misrepresentations, no fine |
| 22 Reynolds Consumer Products, Inc., FTC File No. 1423030 | June 25, 2014 | Certification Lapsed | settled: prohibition from further misrepresentations, no fine |
| 23 Receivables Management Services Corporation, FTC File No. 1423031 | June 25, 2014 | Certification Lapsed | settled: prohibition from further misrepresentations, no fine |
| 24 Tennessee Football, Inc., FTC File No. 1423032 | June 25, 2014 | Certification Lapsed | settled: prohibition from further misrepresentations, no fine |

⁴⁶ Compare cases C-518/07, Commission v. Germany of 9 March 2010 and case C-614/10, European Commission v. Republic of Austria of 16 Oct. 2012, Case C-288/12, European Commission v Hungary of 8 April 2014 in which the Court of Justice clarified that the mere risk of influence being exercised over supervisory authorities is enough to violate the independency requirement.

⁴⁷ Compare figure 1; there is one case in 2012 in which google paid 22, 5 Million Dollar to settle FTC charges, however, these charges were not related to a safe harbor violation, compare: <http://www.ftc.gov/news-events/press-releases/2012/08/google-will-pay-225-million-settle-ftc-charges-it-misrepresented>.

V. FINAL REMARKS

The comparison between the guarantees of SH and Directive 95/46 shows considerable differences concerning the protected rights of individuals. In particular, the self-certifying mechanism and the applicability of US law when it comes to questions of interpretation of SH lead to a lack of protection for EU citizens if their data is transferred under SH. As every rule of the federal, state or even the local level existing in the US can override the guarantees of the SHD, there is no comprehensive protection for the rights of individuals in SH.

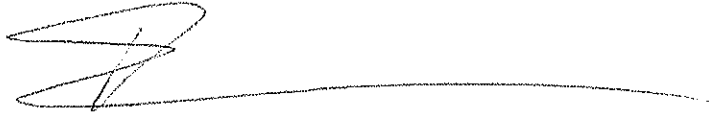
Comparing the enforcement mechanisms of Directive 95/46 and the SH rules, doubts arise regarding the effective enforcement of remedies, sanctions and notification duties as well as the establishment of independent supervisory bodies within the SH framework. It is very doubtful whether the limited jurisdiction of the FTC and the ADR mechanism, which faces various difficulties, can be classified as adequate according to the criteria mentioned in Article 25 (2) of Directive 95/46. The lack of independent and active control over data processing activities is also in contrast to established EU law.

The rules on onward transfer allow for a wide ranging use of data outside the “sphere of protection” of SH. Restrictions and limitations of the fundamental rights of EU citizens go far beyond of what is tolerated in the EU. Such limitations do not even require a proportionality or balancing test between the different interests at stake. This constitutes a clear violation of Article 7, 8 and 52 (1) CFR and the ECHR and can therefore not be regarded as adequate.

Crucial elements with regard to data quality such as fairness, lawfulness, adequacy, explicit purpose limitation that result from Directive 95/46, Article 7, 8 CFR and Article 8 ECHR are not applied at all or applied in a less strict way. Legitimate processing depends on the notice and choice principles which are limited in its application and can also be overridden by US law.

In addition, the rights to deletion, correction and amendment are limited to data that is “inaccurate”. In contrast to EU law, the rights do not refer to data that is processed illegally or in violation of the SH rules. This clearly limits the possibility of the individual to remedy data that may be illegally processed or processed against the rules of SH. Moreover, there is no possibility to obtain access, erasure, rectification or blocking of data that is accessed by US surveillance programs or transferred to others due to other legal obligations mentioned in the opinion.

In summary, there are serious doubts on the adequacy finding of the SH as it could be observed that the SHD is differing in essential points from minimum European data protection standards that are laid down in Directive 95/46.

A handwritten signature in black ink, consisting of a stylized 'F' followed by a long horizontal stroke.

Signature

Franziska Boehm

The opinion was requested by the applicant. Funding was not provided.